Attack Vectors:

Attack Diversity Included the most common attacks based on the 2016- 17-18 McAfee report, such as Web based, Brute force, DoS, DDoS, Infiltration, Heart-bleed, Bot and Scan covered in this netflow cyber attack dataset. **Network Behavior** as Unusual connections between hosts . Higher than average data transfer **Application Behavior** as Service response time abnormally high . Dropped connections exceed normal.

Attacks fall into four main categories:

- DOS: denial-of-service, e.g. syn flood;
- R2L: unauthorized access from a remote machine, e.g. guessing password;
- U2R: unauthorized access to local super user (root) privileges, e.g., various ``buffer overflow'' attacks;
- probing: surveillance and other probing, e.g., port scanning.

Class attribute

class_attack attribte indicates which type of connections is each instance having : **normal or which attack**. The values it can take are the following: anomaly, dict, dict_simple, eject, eject-fail, ffb, ffb_clear, format, format_clear, format-fail, ftp-write, guest, imap, land, load_clear, loadmodule, multihop, perl_clear, perlmagic, phf, rootkit, spy, syslog, teardrop, warez, warezclient, warezmaster, pod, back, ip-sweep, neptune, nmap, portsweep, satan, smurf and normal.

Categories of class attribute

class_attack	Category
smurf	dos
neptune	dos
back	dos

class_attack	Category
teardrop	dos
pod	dos
land	dos
normal	normal
satan	probe
ipsweep	probe
portswee p	probe
nmap	probe
warezcli ent	r2l
guess_pa sswd	r2l
warezma ster	r2l
imap	r2l

class_attack	Category
ftp_write	r2l
multihop	r2l
phf	r2l
spy	r2l
buffer_overflow	u2r
rootkit	u2r
loadmodule	u2r
perl	u2r

Intrinsic Attributes:

Feature Name	Description	Type
Src_byte	Number of data bytes from source to destination	Discrete
Dst_type	number of data bytes from destination to source	Continuous
Duration	length (number of seconds) of the connection	Continuous
Flag	Normal or error status of the connection. Possible status: SF,S0 -3 ,OTH, REJ, RSTO etc	Discrete
Service	network service on the destination, e.g., http, telnet, etc.	Continuous
Protocol_type	type of the protocol, e.g. tcp, udp, etc.	Discrete
Event_id	Unique Id of the events	Discrete
Class_attack	Which type of connections is each instance having : normal or which attack like syslog, teardrop, warez, warezclient, warezmaster, pod, back, ip- sweep, neptune, nmap, portsweep, satan, smurf etc	Continuous
Land	1 if connection is from/to the same host/port; 0 otherwise	Discrete
Wrong_fragment	Sum of bad checksum packets in a connection	Continuous
Urgent	Number of urgent packets. Urgent packets are packets with the urgent bit activated	Continuous

Sample observation the netflow cyber attack data:

event_id	class_attack	dst_bytes	duration	flag	land	protocol_ type	service	src_bytes	urgent	Wrong fragment
70782	normal	0	2	SF	0	tcp	ftp_data	2194619	0	0
14447	normal	7384	0	SF	0	tcp	http	216	0	0
11241	smurf	0	0	SF	0	icmp	ecr_i	1032	0	0
20636	normal	0	0	SF	0	tcp	ftp_data	879	0	0